

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Mikael Sundstrom et al.      Examiner: Unassigned  
Serial No.: Unassigned      Art Group: Unassigned  
Filing Date: July 16, 2001      Docket No. 150-001

Title: Firewall Apparatus and Method of Controlling Network Data Packet Traffic  
Between Internal and External Networks

---

Hon. Commissioner of Patents and Trademarks  
U.S. Patent and Trademark Office  
Washington, D.C. 20231

**PRELIMINARY AMENDMENT**

Dear Sir:

Prior to examination of the above-identified patent application which is being filed concurrently herewith, please amend the application as follows:

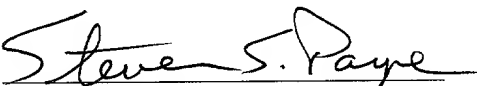
**IN THE CLAIMS**

Please cancel claims 1-14 without prejudice or disclaimer. In addition, please add new claims 15-34 as shown on the attached sheets.

**REMARKS**

Prior to examination, new claims 15-34 have been added to the application to place the application in better form for examination. If the Examiner believes that a telephone interview may expedite the prosecution of the Application, the Examiner is invited to contact the below attorney at the indicated telephone number.

Respectfully submitted,

By:   
Steven S. Payne  
Registration No. 35,316

Date: July 16, 2001

Law Office of Steven S. Payne  
8027 Iliff Drive  
Dunn Loring, VA 22027  
(703) 698-1946  
FAX: (703) 698-1946

We claim:

15. A firewall for controlling network data packet traffic between internal and external networks comprising: filtering means for selecting from a total set of rules, in dependence of the contents in data fields of a data packet being transmitted between said networks a rule applicable to said data packet, in order to block said packet or to forwarded said packet through the firewall, means for look-up in a 2-dimensional table of source and destination addresses of the packet in a set of address prefixes, each address prefix having a subset of rules of the total set of rules, in order to find an address prefix, via its representation, associated with said source and destination addresses, and rule matching means for rule matching - on the basis of the contents of said data fields in order to find the rule applicable to said data packet.

16. A firewall according to claim 15, wherein said means for look-up in a 2-dimensional table comprises means for finding the prefix associated with said source and destination addresses by determining the closest dominating point  $p$  in  $\mathbf{p}$  under the norm  $L_\infty$ , i.e. the dominating point of  $p_i \in \mathbf{p}$  of  $p$  minimising the  $L_\infty$ -distance between  $p_i$  and  $p$ .

25

17. A firewall according to claim 16, wherein the source and destination addresses are represented by a point  $(s,d) \in \mathbf{U}$ , wherein  $\mathbf{U}$  is a 2-dimensional address space represented by integer pairs  $(s,d)$  satisfying:

30  $0 \leq s < 2^{32}$ ,  $0 \leq d < 2^{32}$ ,

the prefixes  $\mathbf{P} = \{P_1, P_2, \dots, P_n\}$  is a partition of the address space  $\mathbf{U}$ , and

each prefix  $P_i$  is a logical rectangle  $R$  in the address space  $\mathbf{U}$  defined by  $[(s_0, d_0), (s_1, d_1)]$ , where  $s_1 - s_0 =$

$s_1 - 2^{1s} * k_s = 2^{1s}$  and  $d_1 - d_0 = d_1 - 2^{1d} * k_d = 2^{1d}$  for some non negative integers  $i_s, i_d, k_s$ , and  $k_d$ ,

said logical rectangle  $R$  being a subset of  $U$  satisfying:  $(s, d) \in R$  if  $s_0 \leq s < s_1$ ,  $d_0 \leq d < d_1$ , wherein  
5  $(s_0, d_0), (s_1, d_1) \in U$ , and the pair of points  $[(s_0, d_0), (s_1, d_1)]$  uniquely defines said rectangle  $R$ .

18. A firewall according to claim 16, wherein  
for each prefix  $P = [(s_0, d_0), (s_1, d_1)] \in P$ , the point  
10  $p_0 = (s_0, d_0)$  is a representative of  $P$ , and  $p = \{p_1, p_2, \dots$   
 $\dots, p_n\} = \{(s_1, d_1), (s_2, d_2), \dots, (s_n, d_n)\}$  is the set of  
representatives of the prefixes in  $P$ , wherein given a point  
 $(s_d, d_d) \in U$ , for each  $(s, d) \in U$ , wherein  $s_d \geq s$  and  $d_d \geq d$ ,  
 $(s, d)$  is dominated by  $(s_d, d_d)$ .

15

19. A firewall according to claim 17, wherein, given  
a pair of points  $(s_1, d_1), (s_2, d_2) \in U$ , the distance between  
the points under the norm  $L_\infty$  is given by:

20 
$$\lim_{k \rightarrow \infty} \sqrt[k]{|s_1 - s_2|^k + |d_1 - d_2|^k} = \max(|s_1 - s_2|, |d_1 - d_2|).$$

20. A firewall according to claim 15, further  
comprising a fragment machine comprising fragment  
25 collecting means for collecting packet fragments from a  
fragmented packet until a fragment header of said packet is  
received, fragment header storing means for storing in an  
entry means information present in a fragment header field  
of the packet, fragment forwarding means for forwarding  
30 packet fragments provided with fragment header information  
starting with the fragment header, wherein each fragment is  
processed by the filtering means as a regular unfragmented  
packet.

21. A firewall according to claim 15, further comprising network address translation means for translating, in dependence of the information in the prefix, internal source addresses to external source  
5 addresses of a packet transmitted out through the firewall, or external source addresses to internal source addresses of a packet transmitted in through the firewall.

22. A firewall according to claim 15, further  
10 comprising network address translation means for translating, in dependence of the information in the prefix internal source addresses to external source addresses of a packet transmitted from the internal network to the external network, or external source addresses to internal  
15 source addresses of a packet transmitted from the external network to the internal network.

23. A firewall according to claim 15, further comprising hole punching means for determining, on the  
20 basis of the information in the prefix, if said packet is subject to a temporary exception from an external-to-internal blocking rule for a connection initiated from the internal network, wherein a return channel for packets transmitted from the external network to the internal  
25 network is established through the firewall during the lifetime of the connection.

24. A firewall for controlling network data packet traffic between internal and external networks, comprising:  
30 filtering means for selecting from a total set of rules, in dependence of the contents in data fields of a data packet being transmitted between said networks, a rule applicable to the data packet, in order to block said packet or to forwarded the packet through the firewall; a fragment  
35 machine comprising fragment collecting means for collecting



storing in an entry means information present in a  
fragment header field of the packet, and

forwarding packet fragments provided with fragment  
header information starting with the fragment header,  
5 wherein each fragment is processed by the filtering means  
as a regular unfragmented packet.

27. A method according to claim 25, wherein the step  
of performing a rule matching it comprises the further step  
10 of:

in dependence of the information in the prefix,  
translating the external source address to an internal  
source address of a packet to be transmitted in through the  
firewall.

15

28. A method according to claim 25, wherein the step  
of performing a rule matching it comprises the further step  
of:

depending on the information in the prefix,  
20 translating the external source address to an internal  
source address of a packet to be transmitted from the  
external network to the internal network.

29. A method according to claim 25, further  
25 comprising the step of:

depending on the information in the prefix  
translating the internal source address to an external  
source address of a packet to be transmitted out through  
the firewall.

30

30. A method according to claim 25, further  
comprising the step of:

depending on the information in the prefix  
translating the internal source address to an external



33. A method according to claim 25, wherein the step  
of performing a 2-dimensional lookup of the source and  
destination addresses of the packet comprises the further  
5 step of:

finding the closest dominating point  $p$  in  $\mathbf{p}$  under the  
norm  $L_\infty$ , i.e. the dominating point of  $p_1 \in \mathbf{p}$  of  $p$ , which  
minimises the  $L_\infty$ -distance between  $p_1$  and  $p$ .

10 34. A method according to claim 33, wherein  
the source and destination addresses are represented  
by a point  $(s,d) \in \mathbf{U}$ , wherein  $\mathbf{U}$  is a 2 dimensional address  
space represented by integer pairs  $(s,d)$  satisfying:

$$0 \leq s < 2^{32}, \quad 0 \leq d < 2^{32},$$

15 the set of prefixes  $\mathbf{P} = \{P_1, P_2, \dots, P_n\}$  is a partition of  
the address space  $\mathbf{U}$ ,

each prefix  $P_1$  is a logical rectangle  $R$  in the  
address space  $\mathbf{U}$  defined by  $[(s_0, d_0), (s_1, d_1)]$ , where  $s_1 - s_0 =$   
 $s_1 - 2^{i_s} * k_s = 2^{i_s}$  and  $d_1 - d_0 = d_1 - 2^{i_d} * k_d = 2^{i_d}$  for some non  
20 negative integers  $i_s, i_d, k_s$ , and  $k_d$ , wherein the logical  
rectangle  $R$  is a subset of  $\mathbf{U}$  satisfying:  $(s,d) \in R$  if  $s_0 \leq$   
 $s < s_1$ ,  $d_0 \leq d < d_1$ , wherein  $(s_0, d_0), (s_1, d_1) \in \mathbf{U}$ , and the  
pair of points  $[(s_0, d_0), (s_1, d_1)]$  uniquely defines said  
rectangle  $R$ ,

25 for each prefix  $P = [(s_0, d_0), (s_1, d_1)] \in \mathbf{P}$ , the point  
 $(s_0, d_0)$  is a representative of  $P$ , and  $\mathbf{p} = \{p_1, p_2, \dots, p_n\}$   
 $= \{(s_1, d_1), (s_2, d_2), \dots, (s_n, d_n)\}$  are the set of representatives  
of the prefixes in  $\mathbf{P}$ , wherein given a point  $(s_d, d_d) \in \mathbf{U}$ ,  
for each  $(s,d) \in \mathbf{U}$ , wherein  $s_d \geq s$  and  $d_d \geq d$ ,  $(s,d)$  is  
30 dominated by  $(s_d, d_d)$ , and

given a pair of points  $(s_1, d_1), (s_2, d_2) \in \mathbf{U}$ , the  
distance between the points under the norm  $L_\infty$  is given by:

$$\lim_{k \rightarrow \infty} \sqrt[k]{|s_1 - s_2|^k + |d_1 - d_2|^k} = \max(|s_1 - s_2|, |d_1 - d_2|).$$